AMENDMENTS TO THE CLAIMS:

This listing of claims replaces all prior versions and listings of claims in the application:

LISTING OF CLAIMS:

1. (Currently Amended) ~~Method~~ A method for checking a digital signature, involving a microcircuit ~~(53) that can be connected~~ connectable to a data processing system ~~(51)~~, the microcircuit being designed to receive requests to check digital signatures from the data processing system, and to process these requests, a digital signature being generated using a private key only known to a signatory entity and associated with a public key,

~~characterized in that it includes~~ said method comprising a step of storing a certificates table ~~(5, 5')~~ containing a digest form of at least one public key in a memory in the microcircuit ~~(53)~~, and a phase ~~(2)~~ of checking a digital signature comprising steps ~~consisting~~ of:

[[-]] receiving ~~(21)~~ by the microcircuit ~~the~~ a digital signature ~~($Sig(Ai_p,M)$)~~ to be checked and a public key ~~($A1_p$)~~ in a pair of keys comprising a private key that was used to generate the digital signature to be checked,

[[-]] calculating ~~(22)~~ a digest form ~~($Hash(A1_p)$)~~ of the received public key, and searching ~~(23)~~ for the calculated digest form of the public key in the certificates table ~~(5, 5')~~, and

[[-]] decrypting ~~(25)~~ the digital signature using the received public key if the calculated digest form of the public key is located in the certificates table.

2. (Currently Amended) ~~Method~~ The method according to claim 1,

~~characterized in that it comprises~~ further comprising a phase ~~(1)~~ of inserting a public key ~~(B_p)~~ into the certificates table ~~(5, 5')~~, comprising steps ~~consisting~~ of:

[[-]] receiving ~~(10)~~ by the microcircuit ~~(53)~~ a certificate ~~(<R,B>)~~ of the public key ~~(B_p)~~ to be inserted in the certificates table, and a public key ~~(R_p)~~ from a certification entity that generated the certificate, the certificate comprising the public key to be added into the certificates table and a digital signature of the certification entity, generated using a private key belonging to a pair of keys including the public key of the certification entity,

[[-]] calculating ~~(11)~~ by the microcircuit a digest form ~~($Hash(R_p)$)~~ of the public key ~~(R_p)~~ received from the certification entity, and searching ~~(12)~~ for the calculated digest form of the public key in the certificates table,

[[-]] decrypting ~~(14)~~ the digital signature using the public key received from the certification entity if the calculated digest form of the public key is located in the table,

[[-]] extracting ~~(17)~~ the public key ~~(B_p)~~ to be inserted from the certificate if the decrypted digital signature is correct,

[[-]] calculating ~~(18)~~ a digest ~~(Hash(B_p))~~ of the public key ~~(B_p)~~ extracted from the certificate, and inserting ~~(19)~~ the calculated digest in the certificates table.

3. (Currently Amended) ~~Method~~The method according to claim 2,

~~characterized in that~~ wherein the phase ~~(1)~~ of inserting a public key ~~(B_p)~~ in the certificates table ~~(5, 5')~~ comprises ~~the insertion~~ a step of inserting in the certificates table of a pointer ~~(8)~~ to the digest of the public key ~~(R_p)~~ of the certification entity that issued the certificate ~~(<R,B>)~~ of the public key to be inserted, so as to define a certification tree in combination with the inserted digest of the public key.

4. (Currently Amended) ~~Method~~The method according to claim 3,

~~characterized in that it includes~~ further comprising a phase ~~(3)~~ of deleting a digest ~~(Hash(B_p))~~ of a public key ~~(B_p)~~ from the certificates table ~~(5, 5')~~, ~~consisting~~ comprising steps of deleting from the certificates table the digest of a public key to be removed ~~from the certificates table~~, and deleting from the certificates table all digests of public keys associated with a pointer ~~(8)~~ indicating the public key ~~(B_p)~~ to be removed, ~~from the certificates table~~.

5. (Currently Amended) ~~Method~~The method according to ~~one of claims~~ claim 2 ~~to 4~~,

~~characterized in that~~ wherein each public key digest entered into the certificates table ~~(5, 5')~~ is associated with a validity end date ~~(7)~~, ~~and in that~~ the phase ~~(1)~~ of inserting a public key ~~(B_p)~~ into the certificates table ~~also comprises~~ further comprising steps ~~consisting~~ of reading in a received certificate a validity end date of the public key to be inserted ~~in the received certificate (<R,B>)~~, and entering the validity end date of the public key ~~(B_p)~~ to be inserted into the certificates table, together with the digest of the public key to be inserted, if it is earlier than the validity end date of the public key ~~(R_p)~~ of the certification entity read in the certificates table.

6. (Currently Amended) ~~Method~~The method according to ~~one of claims~~ claim 2 ~~to 5~~,

~~characterized in that~~ wherein each digest of a public key entered in the certificates table ~~(5, 5')~~ is associated with a usage counter ~~(41)~~ that is incremented every time that a digital signature is checked using the public key, and ~~in that it includes~~ said method comprising deletion of a public key digest from the certificates table when the usage counter is zero and the number of empty locations in the certificates table is less than a predetermined threshold.

7. (Currently Amended) ~~Method~~The method according to ~~one of claims~~ claim 2 ~~to 6~~, ~~characterized in that~~ wherein each public key digest entered into the certificates table ~~(5, 5')~~ is associated with a usage counter ~~(41)~~ that is incremented every time that a digital signature is checked using the public key, ~~on~~ and with a last usage date ~~(42)~~ that is updated every time that the associated usage counter is incremented, ~~and in that when the number of empty locations in the certificates table is less than a predetermined threshold, it also includes~~ said method further comprising a step to select a digest of a public key to be deleted as a function of the corresponding associated values of the usage counter and the last usage date when the number of empty locations in the certificates table is less than a predetermined threshold.

8. (Currently Amended) ~~Method~~The method according to ~~one of claims~~ claim 1 ~~to 7~~, ~~characterized in that~~ wherein the microcircuit ~~(53)~~ uses a predefined hashing function to calculate the digest forms of the public keys.

9. (Currently Amended) ~~Method~~The method according to ~~one of claims~~ claim 1 ~~to 8~~, ~~characterized in that it comprises~~ further comprising a phase of inserting a root public key ~~(R_p)~~ in the certificates table ~~(5, 5')~~, this insertion phase being done by a write processing controlled by a MAC calculated using a specific key in the microcircuit ~~(53)~~ and only known to ~~a transmitting~~ an entity ~~in~~ having issued the microcircuit.

10. (Currently Amended) ~~Method~~The method according to ~~one of claims~~ claim 1 ~~to 9~~, ~~characterized in that~~ wherein the digest of a public key memorized in the certificates table ~~(5, 5')~~ is obtained by calculating a digest of the public key associated with other information such as the validity end date of the public key, identity information and serial numbers, this information being transmitted to the microcircuit ~~(53)~~ every time that the signature is checked using the public key.

11. (Currently Amended) ~~Method~~The method according to ~~one of claims~~ claim 1 ~~to 10~~, ~~characterized in that~~ wherein the digest of a public key memorized in the certificates table ~~(5, 5')~~ is obtained by calculating a digest of the certificate received by the microcircuit ~~(53)~~ when the public key is inserted in the certificates table, this certificate being transmitted to the microcircuit every time that the signature is checked using the public key.

12. (Currently Amended) ~~Method~~The method according to ~~one of claims~~ claim 1 ~~to 11~~, ~~characterized in that~~ wherein the certificates table ~~(5, 5')~~ is stored in a secure memory area in the microcircuit ~~(53)~~.

13. (Currently Amended) ~~Card provided with a~~ A microcircuit ~~(53), characterized in that it uses the method according to one of claims 1 to 12~~ designed to receive requests to check digital signatures from a data processing system, and to process these requests, a digital signature being generated using a private key only known to a signatory entity and associated with a public key, said microcircuit comprising:

memory means for storing a certificates table containing a digest form of at least one public key,

means for receiving a digital signature to be checked and a public key in a pair of keys comprising a private key that was used to generate the digital signature to be checked,

means for calculating a digest form of the received public key, and for searching for the calculated digest form of the public key in the certificates table, and

means for decrypting the digital signature using the received public key if the calculated digest form of the public key is located in the certificates table.

14. (Canceled)

15. (New) The microcircuit according to claim 13,

further comprising:

means for receiving a certificate of the public key to be inserted in the certificates table, and a public key from a certification entity that generated the certificate, the certificate comprising the public key to be added into the certificates table and a digital signature of the

certification entity, generated using a private key belonging to a pair of keys including the public key of the certification entity,

means for calculating a digest form of the public key received from the certification entity, and for searching for the calculated digest form of the public key in the certificates table,

means for decrypting the digital signature using the public key received from the certification entity if the calculated digest form of the public key is located in the table,

means for extracting the public key to be inserted from the certificate if the decrypted digital signature is correct,

means for calculating a digest of the public key extracted from the certificate, and for inserting the calculated digest in the certificates table.

16. (New) The microcircuit according to claim 15,

further comprising means for inserting in the certificates table a pointer to the digest of the public key of the certification entity that issued the certificate of the public key to be inserted, so as to define a certification tree in combination with the inserted digest of the public key.

17. (New) The microcircuit according to claim 16,

further comprising means for deleting from the certificates table a digest of a public key to be removed, and means for deleting from the certificates table all digests of public keys associated with a pointer indicating the public key to be removed.

18. (New) The microcircuit according to claim 15,

further comprising: means for reading in a received certificate a validity end date of a public key to be inserted, and means for entering the validity end date of the public key to be inserted into the certificates table, together with the digest of the public key to be inserted, if the validity end date is earlier than the validity end date of the public key of the certification entity read in the certificates table.

19. (New) The microcircuit according to claim 15,

further comprising means for incrementing a usage counter associated with each public key digest entered into the certificates table, every time that a digital signature is checked using the public key, and means for deleting a public key digest from the certificates table when the

associated usage counter is zero and the number of empty locations in the certificates table is less than a predetermined threshold.

20. (New)The microcircuit according to claim 19,

further comprising means for updating a last usage date associated with each public key digest entered into the certificates table, every time that a digital signature is checked using the public key, means for deleting a public key digest from the certificates table when the number of empty locations in the certificates table is less than a predetermined threshold, and means for selecting a digest of a public key to be deleted as a function of the corresponding associated values of the usage counter and the last usage date.

21. (New)The microcircuit according to claim 13,

further comprising means for executing a predefined hashing function to calculate the digest forms of the public keys.

22. (New)The method according to claim 13,

further comprising means for inserting a root public key in the certificates table, using a write processing controlled by a MAC calculated using a specific key in the microcircuit and only known to an entity having issued the microcircuit.

23. (New)The method according to claim 13,

wherein the means for calculating the digest of a public key memorized in the certificates table comprise means for calculating a digest of the public key associated with other information comprising the validity end date of the public key, identity information and serial numbers, this information being transmitted to the microcircuit every time that the signature is checked using the public key.

24. (New)The method according to claim 13,

wherein the means for calculating the digest of a public key memorized in the certificates table comprise means for calculating a digest of the certificate received by the microcircuit when the public key is inserted in the certificates table, this certificate being transmitted to the microcircuit every time that the signature is checked using the public key.

25. (New)The method according to claim 13, wherein the memory means for storing the certificates table is a secure memory area.